Remarks

Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are pending and rejected. Claims 1, 10 and 29 are amended to correct a grammatical error.

The Examiner repeated the rejection of Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication 2002/0004848 ("Droge") and *Applied Cryptography*, 2nd Edition ("Schneider"), the Examiner relying on Schneider to show features inherent in the Data Encryption Standard ("DES"). In response to Applicants' Amendment of February 24, 2006, the Examiner states:

> In reponse to the Applciant's arguments on page 9 concerning Droge's alleged failure to disclose wherein the second encryption algorithm is applied in a manner such that the data packet is encrypted at the other end other wireless link and prior to the gateway forwarding to the wide area network, the Examiner respectfully disagrees and calls the Applicant's attention to paragraphs 12-13, 36-37, and 42 wherein it is clearly stated:
>
> * * *
>
> It is clear from paragraphs 36-37 and 42 of Droge that the transmission between the first and second interface devices could very well comprise a wired or wireless network (par 36), and that the second interface device may comprise a transmission mechanism for the transmission of the data, now only once encrypted, over a transmission medium (par 37), which might be a PSTN or other type of dedicated communication link such as an ISDN, DSL, T1, dedicated wirelss connection or the like (par 42).
>
> (emphasis added)

Applicants respectfully traverse the Examiner's rejection. The Examiner has apparently overlooked the fact that Claim 1 does not recite sending singly encrypted data over a dedicated link. Instead, Claim 1 recites the second encryption algorithm is applied in a

manner such that the data packet is decrypted at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network:

> 1. A method for transmitting data over a wireless link to a gateway providing access to a wide area network, the method comprising:
>
> encrypting a payload according to a first encryption algorithm;
>
> adding a header to the encrypted payload to form a data packet;
>
> encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secured communications over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and
>
> transmitting the encrypted data packet over the wireless link to the gateway.
>
> (emphasis added)

As the Examiner recognizes in her response to Applicant's arguments, Droge's singly encrypted data traverse only over a dedicated communication link. In fact, at paragraph [0010] Droge specifically rejects sending a singly encrypted data packet over a wide area network:

> Other attempts for providing secure transmission of data over communication networks implement data encryption prior to transmission over a public network. ... Although such protocols currently provide high levels of security (some supporting 128-bit encryption and higher), the rapid advances in processing technology will soon make such protocols easy to compromise. Furthermore, the aforementioned protocols do not prevent a hacker from determining that data is being transmitted and, possibly, observing how much data is being transmitted, which information may be valuable in itself. Accordingly, such protocols can provide only limited security.

The Examiner's reading of Droge on Applicants' Claim 1 ignores Droge's teachings to send doubly encrypted data on all segments that are over non-dedicated communication links. Under Droge's scheme, such as shown in Droge's Figs. 3, 5 and 6, and explained in the accompanying text, data is always transmitted over the wide area network twice-encrypted. To modify Droge such that data is encrypted only once would defeat Droge's purpose, which is to provide additional security in data transmitted over the wide area network. Accordingly, Applicants respectfully submit that Claim 1 and its dependent Claims 2-4 are each allowable over Droge, as Droge teaches against decrypting a doubly encrypted data packet and sending the resulting singly encrypted data packet over a wide area network. Likewise, as independent Claims 6, 10 and 29 each recite a similar limitation, Claims 6, 10 and 29 and their respective dependent Claims 8-9, 11, 15-17, 20, 25-27 and 30-35 are each allowable over Droge. Reconsideration and allowance of Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are therefore requested.

Accordingly, all pending claims (i.e., Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35) are believed allowable and their allowance respectfully requested. If the Examiner has any question regarding the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant at 408-392-9250.

Respectfully submitted,

Edward C. Kwok
Attorney for Applicant(s)
Reg. No. 33,938
Law Offices of
MacPherson Kwok Chen & Heid LLP
2033 Gateway Place, Suite 400
San Jose, CA 95110
Tel: (408) 392-9250
Fax: (408) 392-9262